Risk Management Philosophy and Approach

We identify and manage risks to reduce the uncertainty associated with executing our business strategies and maximising opportunities that may arise. Risks can take various forms and can have material adverse impact on our reputation, operations, human resources and financial performance.

We have established a comprehensive Risk Management Framework approved by our Risk Committee. The Risk Management Framework sets out the governance structure for managing risks, our risk philosophy, risk appetite and tolerance levels, our risk management approach as well as risk factors.

In addition, our risk assessment and mitigation strategy are aligned with our Group strategy and is an integral part of the annual business planning and budgeting process.

Governance Structure for Managing Risks

THE BOARD

- Instils culture and approach for risk governance
- Provides oversight of risk management systems and internal controls
- Reviews key risks and mitigation plans
- Determines risk appetite and tolerance
- Monitors exposure

RISK COMMITTEE

- Reviews and recommends risk strategy and policies
- Oversees design, implementation and monitoring of internal controls
- Reviews adequacy and effectiveness of the Group's risk framework
- Monitors the implementation of risk mitigation plans

AUDIT COMMITTEE

- Reviews adequacy and effectiveness of the Group's internal control framework
- Oversees financial reporting risk for the Group
- Oversees internal and external audit processes

MANAGEMENT COMMITTEE

- Implements risk management practices within all business units and functions

RISK MANAGEMENT COMMITTEE

- Supports the Board and Risk Committee in terms of risk governance and oversight
- Sets the direction and strategies to align corporate risk management with the Group's risk appetite and risk tolerance
- Reviews the risk assessments carried out by the business units
- Reviews and assesses risk management systems and tools
- Reviews efficiency and effectiveness of mitigations and coverage of risk exposures

Our Risk Philosophy

Our risk philosophy and risk management approach are based on three key principles:

RISK CENTRIC CULTURE

- Set the appropriate tone at the top
- Promote awareness, ownership and proactive management of key risks
- Promote accountability

STRONG CORPORATE GOVERNANCE STRUCTURE

- Promote good corporate governance
- Provide proper segregation of duties
- Clearly define risk-taking responsibility and authority
- Promote ownership and accountability for risk taking

PROACTIVE RISK MANAGEMENT PROCESS

- Robust processes and systems to identify, quantify, monitor, mitigate and manage risks
- Benchmark against global best practices

Risk Appetite

The Board has approved the following Risk Appetite Statement:

- The Group is committed to delivering value to our shareholders achieved through sustained profitable growth. However, we shall not compromise our integrity, values and reputation by risking brand damage, service delivery standards, severe network disruption or regulatory non-compliance.
- The Group will defend our market leadership position in Singapore and strengthen our market position in Australia and in Asia Pacific through our regional mobile associates. We will continue to pursue business expansion in the emerging markets, including acquiring controlling stakes in the associates, and actively managing the risks.
- The Group is prepared to take measured risks to seek new growth in the digital space by providing global platforms and enablers, targeted at a global footprint, while leveraging our current scale and core strengths.
- The Group targets an investment grade credit rating and dividend payout policy consistent with our stated dividend policy and guidance.

Risk Management

We have established a rigorous and systematic risk review process to identify, monitor, manage and report risks throughout the organisation based on our risk philosophy. Management has primary responsibility for identifying, managing and reporting to the Board the key risks faced by the Group. Management is also responsible for ensuring that the risk management framework is effectively implemented within the business units. The business units are supported by specialised functions such as Regulatory, Legal, Environment, Insurance, Treasury and Credit Management in the management of risks. In addition, we regularly assess the environmental, social and governance risks that exist or emerge in our broader value chain and address them through various corporate sustainability initiatives.

Our key risk management activities also include scenario planning, business continuity/disaster recovery management and crisis planning and management. Close monitoring and control processes, including the use of appropriate key risk and key performance indicators, are implemented to ensure the risk profiles are managed within policy limits.

In addition, we have in place a formal programme of risk and control self-assessment where line personnel are involved in the ongoing assessment and improvement of risk management and controls. The effectiveness of our risk management policies and processes is reviewed on a regular basis and, where necessary, improved. Independent reviews are conducted by third-party consultants regularly to ensure the appropriateness of the risk management framework.

Risk Management Philosophy and Approach

The consultants also report key risks to the Board, as well as provide periodic support and input when undertaking specific risk assessments. Furthermore, the risk management processes facilitate alignment of our strategy and annual operating plan with the management of key risks.

Singtel's Internal Audit (IA) carries out reviews and internal control advisory activities aligned to the key risks in our businesses. This provides independent assurance to the Audit Committee (AC) on the adequacy and effectiveness of our risk management, financial reporting processes, and internal control and compliance systems. In order to provide assurance to the Board, the CEOs of our business units submit an annual report on the key risks and mitigation strategies for their respective businesses to the Risk Committee. Our Group CEO and Group CFO provide a written certification to the Board confirming the integrity of financial reporting, and the efficiency and effectiveness of the risk management, internal control and compliance systems every year.

In the course of their statutory audit, external auditors review our material internal controls to the extent of the scope laid out in their audit plans. Any material non-compliance and internal control weaknesses, together with their recommendations to address them, are reported to the AC. Our Management, with the assistance of Singtel IA, follows up on the external auditors' recommendations as part of their role in reviewing our system of internal controls.

The systems that are in place are intended to provide reasonable but not absolute assurance against material misstatements or loss, as well as ensuring the safeguarding of assets, the maintenance of proper accounting records, the reliability of financial information, compliance with applicable legislation, regulations and best practices, and the identification and management of business risks.

Risk Factors

Our financial performance and operations are influenced by a vast range of risk factors. Many of these affect not just our businesses, but also other businesses in and outside the telecommunications industry. These risks vary widely and many are beyond the Group's control. There may also be risks that are either presently unknown or not currently assessed as significant, which may later prove to be material. However, we aim to mitigate the exposures through appropriate risk management strategies and internal controls.

The section below sets out the principal risk types, which are not listed in the order of significance.

- Economic Risks
- Political Risks
- Regulatory Risks and Litigation Risks
- Competitive Risks
- Expansion Risks
- Project Risks
- New Business Risks
- Technology Risks
- Vendor/Supply Chain Risks
- Information Technology Risks
- Cyber Security Risks
- Breach of Privacy Risks
- Financial Risks
- Electromagnetic Energy Risks
- Network Failure and Catastrophic Risks
- Talent Management Risks

ECONOMIC RISKS

Changes in domestic, regional and global economic conditions may have a material adverse effect on the demand for telecommunications, information technology (IT) and related services, digital services, and hence, on our financial performance and operations.

The global credit and equity markets have experienced substantial dislocations, liquidity disruptions and market corrections. These and other related events have had a significant impact on economic growth as a whole and consequently, on consumer and business demand for telecommunications, IT and related services, and digital services.

Our planning and management review processes involve the periodic monitoring of budgets and expenditures to minimise the risk of over-investment. Each of the business units in our Group has continuing cost management programmes to drive improvements in their cost structures.

POLITICAL RISKS

Some of the countries in which Group Consumer operates have experienced or continue to experience political instability.

The continuation or re-emergence of such political instability in the future could have a material adverse effect on economic or social conditions in those countries, as well as on the ownership, control and condition of our assets in those areas.

Group Consumer is geographically diversified with operations in Singapore, Australia and the emerging markets. We work closely with the Management and our partners in the countries where we operate to leverage the local expertise, knowledge and ability. This way, we ensure compliance with the laws and are able to implement risk mitigation measures.

As Group Enterprise and Group Digital Life expand their products and services across the region and around the world, exposure to similar political risks may increase in the future.

REGULATORY RISKS AND LITIGATION RISKS

Regulatory Risks

Our businesses depend on licences issued by government authorities. Failure to meet regulatory requirements could result in fines or other sanctions including, ultimately, the revocation of licences. Our global operations are subject to extensive government regulations, which may impact or limit our flexibility to respond to market conditions, competition, new technologies or changes in cost structures. Governments may alter their policies relating to the telecommunications, IT, multimedia and related industries, as well as the regulatory environment (including taxation) in which we operate. Such changes could have a material adverse effect on our financial performance and operations.

Our overseas investments are also subject to the risk of imposition of laws and regulations restricting the level, percentage and manner of foreign ownership and investment, as well as the risk of nationalisation. Any of these factors can materially and adversely affect our overseas investments.

Consumer Australia, Consumer Singapore and Group Enterprise are impacted by the implementation of national broadband networks in both Australia and Singapore. In Singapore, the Infocomm Development Authority of Singapore (IDA) has, in its implementation of the Next Generation Nationwide Broadband Network (Next Gen NBN), designed a structure to level the playing field to make the benefits of the Next Gen NBN available to all industry players. This has significantly altered the existing cost model of the industry and increased the level of competition from new entrants. In Australia, the government is currently undertaking a significant reform of the fixed-line telecommunications sector, including the rollout of a national broadband network (NBN) to be operated on a wholesale-only open access basis. It is possible that the Australian government's regulatory reforms, including legislation and the deployed NBN and commercial transactions relating to the NBN, could ultimately lead to a sub-optimal or negative outcome for Optus.

Our operations are also subject to various other laws and regulations such as those relating to customer data privacy and protection, and workplace safety and health. Failure to meet these regulations may affect our business and/or our capacity to operate in line with our business objectives.

We have access to appropriate regulatory expertise and staffing resources in Singapore and Australia and we work closely with the management and our partners in the countries we operate in. We closely monitor new developments and regularly participate in discussions and consultations with the respective regulatory authorities and the industry to propose changes and provide feedback on regulatory reforms and developments in the telecommunications and media industry.

Access to Spectrum

We may need to access additional spectrum to support both organic growth and the development of new services. Access to spectrum is critically important for supporting our business of providing mobile voice and data. The use of spectrum in most countries where we operate is regulated by government authorities and requires licences. Failure to acquire access to spectrum or new or additional spectrum on reasonable commercial terms or at all could have a material adverse effect on our core communications business, financial performance and growth plans.

Litigation Risks

We are exposed to the risk of regulatory or litigation action by regulators and other parties. Such regulatory matters or litigation actions may have a material effect on our financial condition and results of operations. Examples of such litigation are disclosed in Notes to the Financial Statements under "Contingent Liabilities".

We have put in place standard master supply agreements with vendors and implemented contract policies to manage contractual arrangements with vendors and customers. The policies provide the necessary empowerment framework for the CEOs, the Management Committee and the Board Committees to approve any deviations from the standard policies.

COMPETITIVE RISKS

We face competitive risks in all markets and business segments in which we operate.

Group Consumer Business

The telecommunications market in Singapore is highly competitive. As new players enter the market

Risk Management Philosophy and Approach

and regulation requires Singtel in Singapore to allow our competitors to have access to our networks, our market share in some segments and prices for certain products and services have declined. These trends may continue and intensify.

In the Australian mobile market, in addition to the incumbent operator, a number of participants are subsidiaries of international groups and operators, and have made large investments which are now sunk costs. We are, therefore, exposed to the risk of irrational pricing being introduced by such competitors. The consumer fixed-line services market continues to be dominated by the incumbent provider, which can leverage its scale and market position to restrict the development of competition. With the deployment of the Australian NBN, competition is expected to increase as new operators enter the market.

The operations of our regional mobile associates' businesses are also subject to highly competitive market conditions. Their growth depends in part on the adoption of mobile data services in their markets. Some of these markets have and could continue to experience keen price competition for mobile data services from smaller-scale competitors, leading to lower profitability and potential loss of market share for our associates.

Our business models and profits are also challenged by disintermediation in the telecommunications industry by handset providers and non-traditional telecommunications service providers who provide multimedia content, applications and services directly on demand.

Group Consumer is focused on driving efficiencies and innovation via new technologies, products and services, processes and business models to meet evolving customer needs and strengthen customer loyalty.

Group Enterprise Business
Business customers enjoy wide choices for many of our services, including fixed, mobile, cyber security, cloud, managed services, IT services and consulting. Competitors include multinational IT and telecommunications companies, while in Australia, the enterprise market is dominated by the incumbent. The quality and prices of these services can influence a potential business customer's decision. Prices for some of these services have declined significantly in recent years as a result of capacity additions and price competition. Such price declines are expected to continue.

Group Enterprise continues to focus on offering companies comprehensive and integrated infocomm technology (ICT) solutions and initiatives to strengthen customer engagement. This includes broadening our solution portfolio to cover new areas of customer needs, such as cloud computing, cyber security and solutions for smart cities.

Group Digital Life Business
The digital products and services we offer are primarily in the areas of digital marketing, digital video and data analytics. Competition is intense, with many over-the-top (OTT) operators offering services over the internet and facing low entry barriers.

Group Digital Life aspires to become a significant global player in these areas by delivering distinctive products and services in the target markets and launching them quickly to capture market share. We will continue to harness our valuable assets, such as extensive customer knowledge, touch points, intelligent networks and the scale of our customer base.

EXPANSION RISKS

Given the size of the Singapore and Australia markets, our future growth depends, to a large extent, on our ability to grow our overseas operations in both traditional and new digital services. This comes with considerable risks.

Partnership Relations
The success of our strategic investments depends, to a large extent, on our relationships with, and the strength of our investment partners. There is no guarantee that we will be able to maintain these relationships or that our investment partners will remain committed to their partnerships.

Acquisition Risks
We continually look for investment opportunities that can contribute to our expansion strategy and develop new revenue streams. Our efforts are challenged by the limited availability of opportunities, competition from other potential investors, foreign ownership restrictions, government and regulatory policies, political considerations and the specific preferences of sellers. We face challenges arising from integrating newly acquired businesses with our own operations, managing these businesses in markets where we have limited experience and/or resources and financing these acquisitions. We also risk not being able to generate synergies from these acquisitions, and the acquisitions becoming a drain on our management and capital resources.

The business strategies of some of our regional mobile associates involve expanding operations outside their home countries. These associates may enter into joint ventures and other arrangements with other parties. Such joint ventures and other arrangements involve risks, including, but not limited to, the possibility that the joint venture or investment partner may have economic or business interests or goals that are not consistent with those of the associates. There is no guarantee that the regional mobile associates can generate total synergies and successfully build a competitive regional footprint.

We adopt a disciplined approach in our investment evaluation and decision-making process. Members of our management team are also directors on the boards of our associates. In addition to sharing network and commercial experience, best practices in the areas of corporate governance and financial reporting are also shared across the Group.

PROJECT RISKS

We incur substantial capital expenditure in constructing and maintaining our networks and IT systems infrastructure. These projects are subject to risks associated with the construction, supply, installation and operation of equipment and systems.

The projects that we undertake as contractors to operate and maintain infrastructure are subject to the risks of increased project costs, disputes and unexpected implementation delays, any of which can result in an inability to meet projected completion dates or service levels.

Group Enterprise is a major IT service provider to governments and large enterprises in the region. We face potential project execution risks when projects are not accurately scoped or the quality of service performance is not up to customers' specifications, resulting in over-commitments to customers, as well as inadequate resource allocation and scheduling. These can lead to cost overruns, project delays and losses.

We have a project risk management framework in place, with processes for regular risk assessment, performance monitoring and reporting of key projects.

NEW BUSINESS RISKS

Beyond our traditional carriage business in Singapore and Australia, we are venturing into new growth areas to create additional revenue streams, including mobile applications and services, pay-TV, regional premium OTT video, content, managed services, cloud services, cyber security, ICT, data analytics and digital marketing. There is no assurance that we will be successful in these ventures, which may require substantial capital, new expertise, considerable process or systems changes, as well as organisational, cultural and mindset changes. These businesses may also expose us to new areas of risks associated with the media and online industries such as media regulation, content rights disputes and customer data privacy and protection.

As new businesses place new demands on people, processes and systems, we respond by continually updating our organisation structure, talent management and development programme, reviewing our policies and processes, and investing in new technologies to meet changing needs.

TECHNOLOGY RISKS

Rapid and significant technological changes are typical in the telecommunications and ICT industry. These changes may materially affect Group Consumer and Group Enterprise's capital expenditure and operating costs, as well as the demand for products and services offered by our business divisions.

Rapid technological advances may leave us with infrastructure and systems that are technically obsolete before the end of their expected useful life. Technological changes may also reduce costs and expand the capacities of new infrastructure. In the emerging markets in which our associates operate, regulatory practices, including spectrum availability, may not necessarily synchronise with the technology progression path and the market demand for new technologies. These changes may require us to replace and upgrade our network infrastructure to remain competitive and, as a result, incur additional capital expenditure.

Each business group faces the ongoing risk of market entry by new operators and service providers (including non-telecommunications players) that, by using newer or lower-cost technologies, may succeed in rapidly attracting customers away from established market participants.

Group Enterprise may incur substantial development expenditure to gain access to related or enabling technologies to pursue new growth opportunities in the ICT industry. The challenge is to modify our network infrastructure in a timely and cost-effective manner to facilitate such implementation, failing which this could adversely affect our quality of service, financial condition and results of operations.

We continue to invest in upgrading, modernising and equipping our systems with new capabilities to ensure we continue to deliver innovative and relevant services to our customers.

VENDOR/SUPPLY CHAIN RISKS

We rely on third-party vendors and their extended supply chain in many aspects of our business for various purposes, including, but not limited to, the construction of our network, the supply of handsets and equipment, systems and application development services, content provision and customer acquisition. Accordingly, our operations may be affected by third-party vendors or their supply chain failing to perform their obligations. In addition, the industry is dominated by a few key vendors for such services and equipment, and any failure or refusal by a key vendor to provide such services or equipment, or any consolidation of the industry, may significantly affect our business and operations.

Risk Management Philosophy and Approach

We monitor our relationships with key vendors closely and develop new relationships to mitigate supply risks. We have in place a Sustainable Supply Chain strategy and framework to manage risks that may exist in our extended supply chain.

INFORMATION TECHNOLOGY RISKS

As our businesses and operations rely heavily on information technology, our Management has established the IT & Network Security Committee to provide oversight of all IT and network security risks, including cyber security threats and data privacy breaches. The committee comprises members from the various IT and network domains, meets bi-monthly and reports directly to the Risk Management Committee. The committee develops appropriate policies and frameworks to ensure information system security, reviews the projects and initiatives on IT and network security, and reviews any IT security incidents.

We have established a Group Information Security Policy for managing risks associated with information security in a holistic manner. The policy is developed based on industry best practices and is aligned with international standards such as ISO 27001. The policy covers various aspects of IT risk governance, including change management, user access management, database configuration standards and disaster recovery planning, and provides the cornerstone for driving robust IT security controls across the Group.

We have also established a Project Management Methodology to ensure that new systems are developed with appropriate IT security controls and are subject to rigorous acceptance tests, including penetration testing, prior to implementation.

CYBER SECURITY RISKS

The scale and level of sophistication of cyber security threats have increased especially in recent times. We are exposed to the risks of cyber attacks that can cause disruptions to the network and services provided to customers, and cyber thefts of sensitive and/or confidential information, resulting in litigations from customers and/or regulatory fines and penalties.

To combat these threats, we adopt a holistic approach by keeping abreast of the threat landscape and business environment as well as implementing a multi-layered security framework to ensure there are relevant preventive, detective and recovery measures.

We have developed a security-first mindset and have been building our capabilities organically, through investments as well as partnerships with best-of-breed technology partners to meet the diverse needs of governments and enterprises. Group Enterprise has in September 2015 completed the acquisition of Trustwave, a leading US cyber security services company which enhances the Group's cyber security capabilities. To date, we have over 1,800 security professionals, global security operations and engineering centres as well as a specialised team of ethical hackers and forensic experts in assisting various businesses to manage vulnerabilities and threats, achieve compliance with regulations and implement secure solutions.

BREACH OF PRIVACY RISKS

We seek to protect the privacy of our customers in our networks and systems infrastructure. Significant failure of security measures may undermine customer confidence and materially impact our businesses. We may also be subject to the imposition of additional regulatory measures relating to the security and privacy of customer data.

We have implemented security policies, procedures, technologies and tools designed to minimise the risk of privacy breaches. We have also established an escalation process for major incidents, which includes security breaches, to ensure timely response, internally and externally, to minimise impact.

FINANCIAL RISKS

The main risks arising from our financial assets and liabilities are foreign exchange, interest rate, market, liquidity, access to financing sources and increased credit risks. Financial markets continue to be volatile and this may heighten execution risk for funding activities and credit risk premiums for market participants.

We are exposed to foreign exchange fluctuations from our operations and through subsidiaries as well as associated and joint venture companies operating in foreign countries. These relate to the translation of the foreign currency earnings and carrying values of our overseas operations. Additionally, a significant portion of associated and joint venture company purchases and liabilities are denominated in foreign currencies, versus the local currency of the respective operations. This gives rise to changes in cost structures and fair value gains or losses when marked to market.

We have established policies, guidelines and control procedures to manage and report exposure to such risks. Our financial risk management is discussed further on page 203 in Note 36 to the Financial Statements.

ELECTROMAGNETIC ENERGY RISKS

Health concerns have been raised globally about the potential exposure to Electromagnetic Energy (EME) emissions through using mobile handsets or being exposed to mobile transmission equipment. While there is no substantiated evidence of public health risks from exposure to the levels of EME typically emitted from mobile phones, perceived health risks can be a concern for our customers, the community, and regulators. The perceived health

risks can result in reduced demand for mobile communications or concerns with local communities on the implementation of new mobile base stations which may impact our mobile business and impact revenues or may lead to litigation. In addition, government controls may be introduced to address this perceived risk, restricting our ability to deploy our mobile communications networks.

We design and deploy our network to comply with the relevant Government-mandated standards for exposure to EME. Our standards are based upon those recommended by the International Commission on NonIonizing Radiation Protection (ICNIRP), which is a related agency of the World Health Organisation (WHO). The ICNRP standards are adopted by many countries around the world and are considered best practice. We continue to monitor research findings on EME, health risks and their implications on relevant standards and regulations.

NETWORK FAILURE AND CATASTROPHIC RISKS

The provision of our services depends on the quality, stability, resilience and robustness of our networks and systems. We face the risk of malfunction of, loss of, or damage to, network infrastructure from natural or other uncontrollable events such as acts of terrorism. Some of the countries in which we and/or our regional mobile associates operate have experienced a number of major natural catastrophes over the years, including typhoons, droughts and earthquakes. In addition, other events that are outside our control and/or our regional mobile associates, such as fire, deliberate acts of sabotage, industrial accidents, blackouts, terrorist attacks or criminal acts, could damage, cause operational interruptions or otherwise adversely affect any of the facilities and activities, as well as potentially cause injury or death to personnel. Such losses or damage may significantly disrupt our operations, which may materially adversely affect our ability to deliver services to customers.

We have business continuity plans as well as insurance policies in place. There is a defined crisis management and escalation process for our CEOs and senior management to respond to emergencies and catastrophic events. However, our inability to operate our networks or customer support systems may have a material impact on our business.

TALENT MANAGEMENT RISKS

As we seek new avenues of growth, a key differentiator alongside access to innovation will be the ability to attract and sustain talent including new skills and capabilities. The loss of some or all of our key executives or the inability to attract or retain key talent, could materially and adversely affect our business.

We continue to invest in the skills of our existing workforce and build up our current and emerging capabilities through external professional hires and targeted campus recruitment. In order to develop and retain talent, we conduct regular skills assessment in the critical business areas and set out structured developmental roadmaps to fill new and emerging skills gaps. We have a targeted development approach to cultivate young, emerging and future technical and business leaders through formal learning activities, coaching and mentoring as well as providing critical experiences such as international assignments, rotations and special projects.